

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-202766

(43) 公開日 平成11年(1999) 7月30日

(51) Int.Cl.<sup>8</sup>

G 0 9 C 1/00

H 0 4 L 9/32

識別記号

6 4 0

F I

G 0 9 C 1/00

H 0 4 L 9/00

6 4 0 B

6 7 5 B

審査請求 未請求 請求項の数15 O L (全 15 頁)

(21) 出願番号 特願平10-6629

(22) 出願日 平成10年(1998) 1月16日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 大石 和臣

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

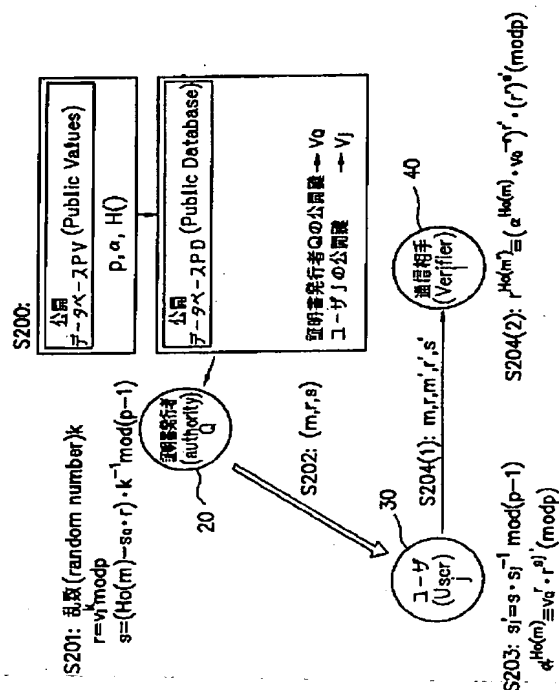
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 デジタル署名方式、それを用いた情報通信システム及び通信装置

(57) 【要約】

【課題】 如何なる場合でも匿名性を確実に保つことができるデジタル署名方式を用いた情報通信システムを提供する。

【解決手段】 手段20は、共通に使用する公開パラメータPVの代わりに、ユーザの公開情報 $v_j$ を用い、デジタル情報 $m$ に対するデジタル署名 $r, s$ を生成する。手段30は、デジタル署名 $r, s$ を秘密情報 $s_j$ を用いて変換することで別の値を求め、デジタル情報 $m$ 、デジタル署名 $r, s$ 、公開パラメータPV、及び公開鍵 $v_Q$ から得られる値を公開情報と見なし、且つ、デジタル署名 $r, s$ を変換して得られた別の値をそのユーザの秘密情報と見なすことで、離散対数問題に安全性の根拠を置く公開鍵暗号を利用する。



# 【特許請求の範囲】

【請求項 1】 各ユーザに共通の公開パラメータ及び各ユーザに固有の秘密情報から、各ユーザに固有の公開情報を生成する公開情報生成ステップと、

デジタル情報に対して上記秘密情報及び上記公開パラメータを用いた変換を施すことで、上記デジタル情報に対応する署名を生成する署名生成ステップと、

上記公開パラメータ及び上記公開情報を用いて、上記デジタル情報と上記署名の対応関係が正しいか否かを判別する署名判別ステップとを含むデジタル署名方式であって、

上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成ステップと、

上記ユーザ情報生成ステップで生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認ステップと、

上記確認ステップで確認された新たなパラメータ及び新たな公開情報を用いて、デジタル情報を暗号化する暗号化ステップとを含むことを特徴とするデジタル署名方式。

【請求項 2】 上記確認ステップで確認された新たなパラメータ及び新たな秘密情報を用いて、上記暗号化ステップで暗号化して得られた暗号文を復号する復号ステップを含むことを特徴とする請求項 1 記載のデジタル署名方式。

【請求項 3】 各ユーザに共通の公開パラメータ及び各ユーザに固有の秘密情報から、各ユーザに固有の公開情報を生成する公開情報生成ステップと、

デジタル情報に対して上記秘密情報及び上記公開パラメータを用いた変換を施すことで、上記デジタル情報に対応する署名を生成する第 1 の署名生成ステップと、

上記公開パラメータ及び上記公開情報を用いて、上記デジタル情報と上記署名の対応関係が正しいか否かを判別する第 1 の署名判別ステップとを含むデジタル署名方式であって、

上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成ステップと、

上記ユーザ情報生成ステップで生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認ステップと、

上記確認ステップで確認された新たなパラメータ及び新たな秘密情報を用いて、デジタル情報に対応する署名を生成する第 2 の署名生成ステップとを含むことを特徴とするデジタル署名方式。

【請求項 4】 上記確認ステップで確認された新たなパラメータ及び新たな公開情報を用いて、上記第 2 の署名生成ステップで生成された署名とそれに対応したデジタル情報の関係が正しいか否かを判別する第 2 の署名判

別ステップを含むことを特徴とする請求項 3 記載のデジタル署名方式。

【請求項 5】 複数のユーザ間で共通に用いられる底の値に対して、各ユーザの秘密情報を指数値として指数計算した結果を、各ユーザの公開情報とする公開情報ステップを含むデジタル署名方式であって、

ユーザの公開情報を共通の底の代わりに用いて生成した平文に対する署名、及び上記ユーザの秘密情報を基に、そのユーザの新たな秘密情報を生成する秘密情報生成ステップと、

上記秘密情報生成ステップで生成された新たな秘密情報に対応する新たなパラメータを生成するパラメータ生成ステップと、

上記署名、上記ユーザの公開情報、上記共通の底、及び上記平文から、上記ユーザの新たな公開情報を生成する公開情報生成ステップと、

上記秘密情報生成ステップで生成された新たな秘密情報、上記パラメータ生成ステップで生成された新たなパラメータ、及び上記公開情報生成ステップで生成された新たな公開情報を用いて、公開鍵暗号を実行する暗号実行ステップとを更に含むことを特徴とするデジタル署名方式。

【請求項 6】 離散対数を求めることの困難性に安全性の根拠を置くデジタル署名方式を含むことを特徴とする請求項 5 記載のデジタル署名方式。

【請求項 7】 上記デジタル署名方式は、ElGamal 署名方式を含むことを特徴とする請求項 6 記載のデジタル署名方式。

【請求項 8】 上記デジタル署名方式は、ElGamal 署名方式の変形を含むことを特徴とする請求項 6 記載のデジタル署名方式。

【請求項 9】 上記公開鍵暗号は、離散対数を求めることの困難性に安全性の根拠を置く暗号を含むことを特徴とする請求項 5 記載のデジタル署名方式。

【請求項 10】 請求項 1～9 の何れかに記載のデジタル署名方式を用いた情報通信システムであって、第 1 のユーザが第 2 のユーザに対して、毎回異なる新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成可能なユーザ情報生成手段と、

上記第 2 のユーザに対する情報が、上記第 1 のユーザが上記ユーザ情報生成手段により生成したものであることを確認するユーザ情報確認手段と、

上記ユーザ情報確認手段で確認された情報を用いて、公開鍵暗号を実行する公開鍵暗号実行手段とを含み、

上記ユーザ情報生成手段により生成された新たなパラメータ、及び新たな公開情報から、それらに対応するユーザが情報量的に判定不可能であることを特徴とする情報通信システム。

【請求項 11】 ユーザに共通の公開パラメータ及びユーザに固有の秘密情報からユーザに固有の公開情報を生

成する公開情報生成手段と、

上記公開パラメータ及び上記公開情報を用いて、送信されてきたデジタル情報と、そのデジタル情報に対応する署名との対応関係が正しいか否かを判別する署名判別手段と、

上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成手段と、

上記ユーザ情報生成手段で生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認手段と、

上記確認手段で確認された新たなパラメータ及び新たな公開情報を用いて、デジタル情報を暗号化する暗号化手段とを備えることを特徴とするデジタル署名方式の通信装置。

【請求項 12】 上記確認手段で確認された新たなパラメータ及び新たな秘密情報を用いて、デジタル情報に対応する署名を生成する署名生成手段を備えることを特徴とする請求項 11 記載の通信装置。

【請求項 13】 複数のユーザ間で共通に用いられる底の値に対して、ユーザの秘密情報を指数値として指数計算した結果を、ユーザの公開情報とする公開情報手段と、

上記公開情報を共通の底の代わりに用いて生成したデジタル情報に対する署名、及び上記秘密情報を基に、新たな秘密情報を生成する秘密情報生成手段と、

上記秘密情報生成手段で生成された新たな秘密情報に対応する新たなパラメータを生成するパラメータ生成手段と、

上記署名、上記公開情報、上記共通の底、及び上記デジタル情報から、新たな公開情報を生成する公開情報生成手段と、

上記秘密情報生成手段で生成された新たな秘密情報、上記パラメータ生成手段で生成された新たなパラメータ、及び上記公開情報生成手段で生成された新たな公開情報を用いて、公開鍵暗号を実行する暗号実行手段とを備えることを特徴とするデジタル署名方式の通信装置。

【請求項 14】 上記デジタル署名方式は、請求項 1～9 の何れかに記載のデジタル署名方式であることを特徴とする請求項 11～13 の何れかに記載の通信装置。

【請求項 15】 請求項 11～14 の何れかに記載の通信装置を含むことを特徴とする情報通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、公開鍵暗号を用いたデジタル署名方式、それを用いた情報通信システム及び通信装置に関するものである。

【0002】

【従来の技術】 例えば、コンピュータと通信ネットワー

クの発展と広範な普及に伴い、従来は通信ネットワーク上で実現できなかった社会的活動等、多様な機能が実現できるようになった。しかしながらその反面、誰が、いつ、どこで、何を行ったのかを容易に把握される場合があった。そこで、これを防ぐために、匿名で通信処理を行うことで、プライバシーを保護し、且つ通信ネットワーク上で多様な機能を実現する方法が提案されている。

【0003】 このような方法としては、例えば、公開鍵暗号を用いた方法があり、これにより、送信者は、通信内容を意図する受信者のみに送信でき、しかも受信者は、受信した通信内容の送信者が誰であるかを確実に確認することが可能となる。そして、この方法を適用したものであることは、特願平 8-108225 号に開示されているデジタル署名方式及びそれを用いた情報通信システムがある。

【0004】 ここで、「暗号」及び「匿名公開鍵証明書」について具体的に説明する。

【0005】 (1) 「暗号」

まず、「暗号」とは、情報の意味が当事者以外には認識できないように情報を変換することをいう。そして、この暗号においては、元の文（変換されていない文）を「平文」といい、その平文を第三者に意味の分からない文（暗号文）に変換することを「暗号化」といい、その変換の手順を「暗号アルゴリズム」という。平文及び暗号文は、テキストデータに限られるものではなく、音声や画像等、あらゆる情報を想定している。暗号化は、「暗号化鍵」と呼ばれるパラメータに依存する変換である。そして、その暗号化で得られた暗号文を当事者が元の平文に戻すことを「復号」といい、その復号の際には、「復号鍵」と呼ばれる暗号化鍵に対応するパラメータが用いられる。一方、当事者以外の第三者が暗号文を元の平文に戻すこと、或いは、復号鍵を見いだすことを「解読」という。

【0006】 上述のような暗号では暗号の安全性を、暗号化に用いる暗号化鍵或いは復号に用いる復号鍵に帰着させており、それらの鍵を知らなければ、たとえ暗号アルゴリズムを知っていても、平文は得られないようになっている。したがって、所定の暗号化を行う装置（暗号装置）の製造者でも、解読不可能な暗号化を実現することができる。

【0007】 また、暗号には、多くの暗号アルゴリズムがある。そこで、例えば、暗号化鍵を公開できるか否かの観点から、暗号を、非対称暗号（公開鍵暗号）と対称暗号（共通鍵暗号）の 2 つに分類して説明する。

【0008】 (1-1) 「非対称暗号（公開鍵暗号）」

「非対称暗号」とは、「公開鍵暗号」とも呼ばれ、暗号化鍵と復号鍵が異なり、暗号化鍵から復号鍵が容易に計算して得られないようになっており、また、暗号化鍵を公開し、復号鍵を秘密に保持して使用される暗号のことをいう。このような非対称暗号は、以下のような特徴を

持っている。

特徴1：暗号化鍵と復号鍵が異なり、暗号化鍵が公開されるため、暗号化鍵を秘密に配送する必要がなく、その鍵の配送が容易である。

特徴2：各利用者の暗号化鍵は公開されるため、各利用者は、各自の復号鍵のみ秘密に保持しておけばよい。

特徴3：送信されてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証（デジタル署名）機能を実現できる。

【0009】ここで、暗号機能と上述の認証機能を実現できる非対称暗号としては、RSA暗号（R.L.Rivest, A.Shamir and L.Adleman, "A method of obtaining digital signatures and public key cryptosystems," Communications of ACM, Vol. 21, No. 2, pp. 120-126, 1978）や、ElGamal暗号（T.E.ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transaction on Information Theory, Vol. IT-31, No. 4, pp. 496-472, 1985）が知られている。また、認証機能を実現できる非対称暗号としては、Fiat-Shamir暗号（A.Fiat, A.Shamir, "How to prove yourself: practical solutions of identification and signature problems," Proc. of CRYPTO' 86, 1987）や、Schnorr暗号（C.P.Schnorr, "Efficient signature generation by smart cards," Journal of Cryptology, vol. 4, pp. 161-174, 1991）が知られている。

【0010】例えば、ElGamal暗号における暗号化、復号、認証（デジタル署名）の生成、及びその検証について具体的に説明する。

【0011】まず、「Z」を整数全体の集合、「 $Z_p$ 」を0以上p未満の整数の集合、「 $Z_p \setminus \{0\}$ 」を $Z_p$ から0を除いた集合、「 $Z_p^*$ 」を $Z_p$ の要素且つpと互いに素である整数の集合として表すものとする。また、整数A、B、Cに対して、

$$A = B \bmod C$$

なる関係が成り立つとき、BをCで割ったときの余りがAであること（任意の整数kが存在し、「 $B = k \cdot C + A$ 」が成り立つこと）を意味し、

$$A \equiv B \pmod{C}$$

なる関係が成り立つとき、AをCで割ったときの余りと、BをCで割ったときの余りとが等しいことを意味するものとする。さらに、通信相手と共通の公開パラメータとしては、素数p、 $Z_p^*$ の要素であり且つ位数p-1の $\alpha$ 、及び一方向性ハッシュ関数 $H_0: Z \rightarrow Z_p \setminus \{0\}$ を用いる。また、任意のユーザiの復号鍵（秘密鍵）を「 $s_i \in Z_{p-1}$ 」とし、暗号化鍵（公開鍵）を「 $v_i = \alpha^{s_i} \bmod p$ 」とする。尚、「一方向性ハッシュ関数」とは、衝突を起こしにくい圧縮関数のことである。すなわち、「一方向性ハッシュ関数」とは、任意の長さのビット列を出力する関数であり、同じ出力となる

入力を見つけることが困難である、という特徴を持っている。

#### 【0012】①暗号化

そこで、ユーザjが平文（メッセージ） $m (\in Z_p)$ を暗号化してユーザiに対して送信する場合、ユーザj用端末装置では、以下のステップ1～ステップ4の手順でその処理が行われる。尚、メッセージmが $Z_p$ の要素でない場合、すなわちp以上の数値の場合には、そのメッセージmを $Z_p$ の要素となるようにブロック分割され、各ブロックに対して、以下の手順の暗号化が行われる。ステップ1：ユーザj用端末装置は、乱数kを生成する。

ステップ2：ユーザj用端末装置は、

$$C_1 = \alpha^k \bmod p$$

なる計算を行う。

ステップ3：ユーザj用端末装置は、

$$C_2 = m \cdot v_i^k \bmod p$$

なる計算を行う。

ステップ4：ユーザj用端末装置は、ステップ2及び3の計算結果 $C_1$ 及び $C_2$ を、ユーザi用端末装置に対して送信する。

#### 【0013】②復号

上記①暗号化により、ユーザj用端末装置からユーザi用端末装置には、 $C_1$ 及び $C_2$ が送信される。そして、ユーザi用端末装置は、ユーザj用端末装置から送信されてきた $C_1$ 及び $C_2$ を用いて、メッセージmを、 $m = C_2 / C_1^{s_i} \bmod p$ なる計算により求める。

#### 【0014】③デジタル署名の生成

上記②復号により得られたメッセージm（ $\in Z$ ）に対して、ユーザi用端末装置がデジタル署名を生成する場合、ユーザi用端末装置では、以下のステップ1～ステップ4の手順でその処理が行われる。尚、上記①暗号化で述べたように、メッセージmをブロック分割する場合もあるが、ここでは、一方向性ハッシュ関数を用いる場合を説明する。

ステップ1：ユーザi用端末装置は、乱数k（ $\in Z_{p-1}^*$ ）を生成する。

ステップ2：ユーザi用端末装置は、

$$r = \alpha^k \bmod p$$

なる計算を行う。

ステップ3：ユーザi用端末装置は、

$$s = (H_0(m) - s_i \cdot r) \cdot k^{-1} \bmod (p-1)$$

なる計算を行う。

ステップ4：ユーザi用端末装置は、ステップ2及び3の計算結果r及びsを、検証者に対して送信する。

#### 【0015】④デジタル署名の検証

そして、上記③デジタル署名の生成により得られたデジタル署名を、ユーザi用端末装置が検証する場合、ユーザi用端末装置は、

$$\alpha^{H_0(m)} \equiv v_j \cdot r \cdot s \pmod{p}$$

なる関係が成り立つか否かを確認する。

【0016】(1-2)「対称暗号(共通鍵暗号)」一方、「対称暗号」とは、「共通鍵暗号」とも呼ばれ、暗号化鍵と復号鍵が同一である暗号のことをいう。また、1970年後半に上述した非対称暗号(公開鍵暗号)が現れてから、従来から存在するこの対称暗号は、「慣用暗号」とも呼ばれるようになった。このような対称暗号は、適当な長さの文字列(ブロック)毎に同じ暗号化鍵で暗号化するブロック暗号と、文字列又はビット毎に暗号化鍵を変えて暗号化するストリーム暗号とに分類される。ブロック暗号としては、文字の順序を置き換えて暗号化する転置式暗号や、文字を他の文字に換える換字式暗号等があり、DES(Data Encryption Standard)や、FEAL(Fast data Encipherment Algorithm)といった商用暗号として広く用いられている。ストリーム暗号は、メッセージに乱数をXOR(排他論理和)して、その内容を攪乱する暗号であり、このストリーム暗号としては、無限周期の乱数列を1回限りの使い捨て鍵として用いるバーナム暗号が知られている。

【0017】尚、上述した(1)暗号の更なる詳細は、「暗号理論入門」(岡本栄司著:共立出版)や、「Applied cryptography second edition: protocols, algorithms, and source code in C」(Schneier著)、「John Wiley & Sons, Inc」等に述べられている。

【0018】(2)「匿名公開鍵証明書」つぎに、「匿名公開鍵証明書」とは、上述した(1-1)非対称暗号(公開鍵暗号)等において、任意のユーザと、そのユーザの公開鍵(暗号化鍵)との対応を保証するものである。具体的には、「Certification Authority」と呼ばれる信頼できる特別なユーザ(以下、CAと言う)が、他のユーザ(以下、ユーザjとする)の身元を、例えば、パスポートで確認し、ユーザjの識別情報ID(氏名、性別、生年月日等の個人識別情報)、その公開鍵及び有効期限等を内容とするメッセージに対するデジタル署名を生成する。このデジタル署名が「匿名公開鍵証明書」である。CAの公開鍵は、誰でも確実に入手できるようになされており、CAにて生成されたデジタル署名を検証することは容易である。これにより、例えば、ユーザkがユーザjと通信する際に、ユーザjに対応する公開鍵を容易に且つ確実に確認することができると共に、他のユーザがユーザjになりすますことを防ぎながら、公開鍵暗号による通信を可能とすることができる。

【0019】また、「匿名公開鍵証明書」とは、上述の匿名公開鍵証明書のユーザが、どこの誰であるかを分らないようにしたものでもある。これにより、プライバシー保護を要する用途、例えば、ある特別なサービスを受けることができる資格を有するが、身元を明かすことを防ぎたい場合に用いることができる。これを適用した

ものとしては、例えば、特願平8-108226号に開示されているグループ署名と呼ばれる特殊なデジタル署名方式がある。

【0020】上述のような匿名公開鍵証明書を適用したものとしては、例えば、特願平8-108225号に開示されている通信システムがある。この通信システムでは、図5に示すようなステップS500~S504の処理が行われる。以下、ステップS500~S504について具体的に説明する。尚、以下の説明における各記号(「Z」や「Z<sub>p</sub>」等)は、上述したElGamal暗号の説明での各記号と同様に定義して用いるものとする。

【0021】ステップS500: 先ず、システム共通の公開パラメータPV(Public Values)としては、素数p、位数q(但し、q | p-1)、Z<sub>p</sub>\*の要素であり且つ位数qのα、一方向性ハッシュ関数H<sub>1</sub>: Z<sub>q</sub> × Z → {0, ..., 2<sup>t</sup>-1}を用いる。すなわち、qは、p-1を割り切り、x ∈ Z<sub>q</sub> \ {0}に対してα<sup>x</sup> ≡ 1 (mod p)ではなく、且つx = qに対してα<sup>x</sup> ≡ 1 (mod p)であり、H<sub>1</sub>は、Z<sub>q</sub>の要素とZの要素を入力とし2<sup>t</sup>-1以下の非負整数を出力する。そして、これらのパラメータは、この通信システムに参加している全てのユーザがアクセスすることができ、且つ不当な改ざん等が起こらないように適切に管理されている公開データベースPD(Public Database)に登録されているものとする。そこで、証明書発行者(authority)Q用端末装置70は、復号鍵(秘密鍵)s<sub>Q</sub>と、暗号化鍵(公開鍵)v<sub>Q</sub>(v<sub>Q</sub> = α<sup>-s<sub>Q</sub></sup> mod p)とを生成し、公開鍵v<sub>Q</sub>を公開データベースPDに登録する。また、ユーザ(User)j用端末装置80は、復号鍵(秘密鍵)s<sub>j</sub>と、暗号化鍵(公開鍵)v<sub>j</sub>(v<sub>j</sub> = α<sup>-s<sub>j</sub></sup> mod p)とを生成し、公開鍵v<sub>j</sub>を公開データベースPDに登録する。

【0022】ステップS501: 匿名公開鍵証明書の生成

次に、証明書発行者Q用端末装置70は、ユーザjの公開鍵v<sub>j</sub>を、乱数(random number)rを用いて変換したzを求め、このzに対する署名(Schnorr暗号によるデジタル署名)を生成する。具体的には、証明書発行者Q用端末装置70は、乱数(秘密の乱数)r

(r ∈ Z<sub>q</sub> \ {0})を選択し、

$$x = \alpha^r \pmod{p}$$

$$z = v_j \cdot r \pmod{p}$$

$$e = H_1(x, z_j)$$

$$y = r + e \cdot s_Q \pmod{q}$$

なる計算を行う。このSchnorr暗号によるデジタル署名(y, e, z)が匿名公開鍵証明書である。

【0023】ステップS502: 匿名公開鍵証明書の配送

次に、証明書発行者Q用端末装置70は、上述のステッ

プS501にて生成した匿名公開鍵証明書 ( $y, e, z$ ) を、ユーザj用端末装置80に対して送信する。これを受けたユーザj用端末装置80は、 $e$ 及び $z$ を、 $e = H_1(\alpha^y \cdot vq^e \bmod p, z)$   
 $z = (\alpha^y \cdot vq^e \bmod p)^{-S_j} \bmod p$   
 が成り立つことを確認する。尚、ここでは、 $x = \alpha^y \cdot vq^e \bmod p$  が成り立つことにより、表記の簡略化のために $x$ を用いるものとする。

【0024】ステップS503：公開鍵暗号の利用  
 次に、ユーザj用端末装置80は、 $\alpha$ と $v_j$ の代わりに $x$ と $z$ を用いて、離散対数問題に基づく公開鍵暗号を利用する。例えば、Schnorr暗号によるデジタル署名を利用する場合、メッセージ $m$ に対して、以下のようしてデジタル署名を生成する。すなわち、ユーザj用端末装置80は、秘密の乱数 $r_j$  ( $r_j \in \mathbb{Z}_q^*$ ) を選択し、  
 $x_j = x^{r_j} \bmod p$   
 $e_j = h(x_j, m)$   
 $y_j = r_j + e_j \cdot s_j \bmod q$   
 なる計算を行う。そして、ユーザj用端末装置80は、メッセージ $m$ と共に、( $y, e, z$ ), ( $y_j, e_j, m$ ) をデジタル署名として、必要な相手に対して送信する。

【0025】ステップS504：署名確認  
 そして、上述のステップS503にて送信されたデジタル署名 ( $(y, e, z), (y_j, e_j, m)$ ) の受信者 (通信相手 (Verifier)) i用端末装置90は、先ず、上述のステップS502における  
 $e = H_1(\alpha^y \cdot vq^e \bmod p, z)$   
 なる式を確認し、次に、  
 $e_j = H_1(x^{y_j} \cdot z^{e_j} \bmod p, m)$   
 なる式を確認する。これらの確認ができた場合に、受信者i用端末装置90は、メッセージ $m$ に対するデジタル署名は証明書発行者Qにより選ばれたユーザによって生成されたデジタル署名である、と認識する。

#### 【0026】

【発明が解決しようとする課題】ところで、上記図5の通信システムで説明したような従来の匿名公開鍵証明書では、匿名性が満たされている。すなわち、任意の匿名公開鍵証明書がどのユーザに対応するものであるのかが分からないようになっている。このような匿名性は、以下の2つの仮定に基づくものである。

#### 【0027】仮定1：離散対数問題

「G」を有限群とし、「 $\alpha$ 」をその生成元とする。また、「 $v$ 」をGの元とし、底Aに対する $v$ の離散対数を「 $\log[\alpha] v$ 」とする。そこで、Gの位数 (元の個数) が充分大きい場合、離散対数 $\log[\alpha] v$ を求めることは困難となる。

#### 【0028】仮定2：離散対数の比較問題

「 $r$ 」と「 $s$ 」をGのランダムな元とする。そこで、

$\alpha, v = \alpha^s, x = \alpha^r, z = \alpha^{rs}$  が与えられたとき、Gの位数が充分大きく、 $r$ と $s$ が未知である場合、 $\log[\alpha] v$ と $\log[x] z$ が等しいか否かを判別することはできない。

【0029】上述のような仮定1及び仮定2が成り立つことにより、匿名公開鍵証明書は匿名性が満たされる。

【0030】しかしながら、従来では、仮定2のみを解くアルゴリズムが見いだされ、仮定1は成り立つが仮定2が成り立たず、匿名公開鍵証明書の匿名性が無くなる場合があった。

【0031】具体的にはまず、仮定1の離散対数問題を解くことは、現在までの研究成果によれば非常に難しいとされ、安全性の根拠として用いることは妥当であると考えられている。すなわち、このような離散対数問題が解ければ、仮定2の離散対数の比較問題も解けることになる。これにより、仮定2を解くことは、仮定1を解くことと同じくらい易しい、或いは、仮定1を解くことよりも易しい、ということがわかる。したがって、この仮定2を解くことが仮定1を解くことよりどの程度易しいかは、現在のところ不明であるが、仮定2のみを解くアルゴリズムが見いだされた場合、仮定1は成り立つが仮定2が成り立たなくなるという事態が考えられる。このような場合に、上述した匿名公開鍵証明書の匿名性が無くなる。

【0032】そこで、本発明は、上記の欠点を除去するために成されたもので、如何なる場合でも匿名性を確実に保つことができるデジタル署名方式、それを用いた情報通信システム及び通信装置を提供することを目的とする。

#### 【0033】

【課題を解決するための手段】本発明は、ElGamal暗号等のデジタル署名を生成する手段と、その手段で生成されるデジタル署名を各ユーザの秘密情報を用いて変換する手段と、離散対数問題に安全性の根拠を置く公開鍵暗号を利用する手段とを少なくとも備えている。この構成において、上記デジタル署名を生成する手段は、共通に使用する公開パラメータの代わりに、各ユーザの公開情報を用い、任意の平文や予め定められた固定値等のデジタル情報に対するデジタル署名を生成する。上記デジタル署名を変換する手段は、上記デジタル署名を各ユーザの秘密情報を用いて変換することで、別の値を求める。上記公開鍵暗号を利用する手段は、上記デジタル情報、上記デジタル署名、上記公開パラメータ、及び署名者の公開鍵から得られる値を公開情報と見なし、且つ、上記デジタル署名を変換して得られた別の値をそのユーザの秘密情報と見なすことで、離散対数問題に安全性の根拠を置く公開鍵暗号を利用する。この公開鍵暗号を利用する手段を用いて、各ユーザは公開鍵暗号を利用する。これにより、各ユーザが公開鍵として用いる情報 (公開情報) から、その情報が

どのユーザと対応するかを特定することが、情報量的に不可能となるため、匿名性は、上述の仮定2（離散対数の比較問題）に依存していない。すなわち、上記仮定2が成り立たなくなる事態が起きたとしても、匿名性は保たれる。

【0034】すなわち、第1の発明は、各ユーザに共通の公開パラメータ及び各ユーザに固有の秘密情報から、各ユーザに固有の公開情報を生成する公開情報生成ステップと、デジタル情報に対して上記秘密情報及び上記公開パラメータを用いた変換を施すことで、上記デジタル情報に対応する署名を生成する署名生成ステップと、上記公開パラメータ及び上記公開情報を用いて、上記デジタル情報と上記署名の対応関係が正しいか否かを判別する署名判別ステップとを含むデジタル署名方式であって、上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成ステップと、上記ユーザ情報生成ステップで生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認ステップと、上記確認ステップで確認された新たなパラメータ及び新たな公開情報を用いて、デジタル情報を暗号化する暗号化ステップとを含むことを特徴とする。

【0035】第2の発明は、上記第1の発明において、上記確認ステップで確認された新たなパラメータ及び新たな秘密情報を用いて、上記暗号化ステップで暗号化して得られた暗号文を復号する復号ステップを含むことを特徴とする。

【0036】第3の発明は、各ユーザに共通の公開パラメータ及び各ユーザに固有の秘密情報から、各ユーザに固有の公開情報を生成する公開情報生成ステップと、デジタル情報に対して上記秘密情報及び上記公開パラメータを用いた変換を施すことで、上記デジタル情報に対応する署名を生成する第1の署名生成ステップと、上記公開パラメータ及び上記公開情報を用いて、上記デジタル情報と上記署名の対応関係が正しいか否かを判別する第1の署名判別ステップとを含むデジタル署名方式であって、上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成ステップと、上記ユーザ情報生成ステップで生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認ステップと、上記確認ステップで確認された新たなパラメータ及び新たな秘密情報を用いて、デジタル情報に対応する署名を生成する第2の署名生成ステップとを含むことを特徴とする。

【0037】第4の発明は、上記第3の発明において、上記確認ステップで確認された新たなパラメータ及び新たな公開情報を用いて、上記第2の署名生成ステップで生成された署名とそれに対応したデジタル情報の関係

が正しいか否かを判別する第2の署名判別ステップを含むことを特徴とする。

【0038】第5の発明は、複数のユーザ間で共通に用いられる底の値に対して、各ユーザの秘密情報を指数値として指数計算した結果を、各ユーザの公開情報とする公開情報ステップを含むデジタル署名方式であって、ユーザの公開情報を共通の底の代わりに用いて生成した平文に対する署名、及び上記ユーザの秘密情報を基に、そのユーザの新たな秘密情報を生成する秘密情報生成ステップと、上記秘密情報生成ステップで生成された新たな秘密情報に対応する新たなパラメータを生成するパラメータ生成ステップと、上記署名、上記ユーザの公開情報、上記共通の底、及び上記平文から、上記ユーザの新たな公開情報を生成する公開情報生成ステップと、上記秘密情報生成ステップで生成された新たな秘密情報、上記パラメータ生成ステップで生成された新たなパラメータ、及び上記公開情報生成ステップで生成された新たな公開情報を用いて、公開鍵暗号を実行する暗号実行ステップとを更に含むことを特徴とする。

【0039】第6の発明は、上記第5の発明において、離散対数を求めることの困難性に安全性の根拠を置くデジタル署名方式を含むことを特徴とする。

【0040】第7の発明は、上記第6の発明において、上記デジタル署名方式は、ElGamal署名方式を含むことを特徴とする。

【0041】第8の発明は、上記第6の発明において、上記デジタル署名方式は、ElGamal署名方式の変形を含むことを特徴とする。

【0042】第9の発明は、上記第5の発明において、上記公開鍵暗号は、離散対数を求めることの困難性に安全性の根拠を置く暗号を含むことを特徴とする。

【0043】第10の発明は、請求項1～9の何れかに記載のデジタル署名方式を用いた情報通信システムであって、第1のユーザが第2のユーザに対して、毎回異なる新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成可能なユーザ情報生成手段と、上記第2のユーザに対する情報が、上記第1のユーザが上記ユーザ情報生成手段により生成したものであることを確認するユーザ情報確認手段と、上記ユーザ情報確認手段で確認された情報を用いて、公開鍵暗号を実行する公開鍵暗号実行手段とを含み、上記ユーザ情報生成手段により生成された新たなパラメータ、及び新たな公開情報から、それらに対応するユーザが情報量的に判定不可能であることを特徴とする。

【0044】第11の発明は、ユーザに共通の公開パラメータ及びユーザに固有の秘密情報からユーザに固有の公開情報を生成する公開情報生成手段と、上記公開パラメータ及び上記公開情報を用いて、送信されてきたデジタル情報と、そのデジタル情報に対応する署名との対応関係が正しいか否かを判別する署名判別手段と、上

記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成手段と、上記ユーザ情報生成手段で生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認手段と、上記確認手段で確認された新たなパラメータ及び新たな公開情報を用いて、デジタル情報を暗号化する暗号化手段とを備えることを特徴とする。

【0045】第12の発明は、上記第11の発明において、上記確認手段で確認された新たなパラメータ及び新たな秘密情報を用いて、デジタル情報に対応する署名を生成する署名生成手段を備えることを特徴とする。

【0046】第13の発明は、複数のユーザ間で共通に用いられる底の値に対して、ユーザの秘密情報を指数値として指数計算した結果を、ユーザの公開情報とする公開情報手段と、上記公開情報を共通の底の代わりに用いて生成したデジタル情報に対する署名、及び上記秘密情報を基に、新たな秘密情報を生成する秘密情報生成手段と、上記秘密情報生成手段で生成された新たな秘密情報に対応する新たなパラメータを生成するパラメータ生成手段と、上記署名、上記公開情報、上記共通の底、及び上記デジタル情報から、新たな公開情報を生成する公開情報生成手段と、上記秘密情報生成手段で生成された新たな秘密情報、上記パラメータ生成手段で生成された新たなパラメータ、及び上記公開情報生成手段で生成された新たな公開情報を用いて、公開鍵暗号を実行する暗号実行手段とを備えることを特徴とする。

【0047】第14の発明は、上記第11～13の何れかの発明において、上記デジタル署名方式は、請求項1～9の何れかに記載のデジタル署名方式であることを特徴とする。

【0048】第15の発明は、請求項11～14の何れかに記載の通信装置を含むシステムであることを特徴とする。

【0049】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。

【0050】まず、第1の実施の形態について説明する。

【0051】本発明に係るデジタル署名方式は、例えば、図1に示すような通信システム100により実施され、この通信システム100は、本発明に係る情報通信システムを適用したものである。

【0052】すなわち、通信システム100では、証明書発行者Q用端末装置20と、ユーザj、i、kを含む複数のユーザ用端末装置30、40、50、・・・とがネットワーク10上で接続されており、各端末装置は、ネットワーク10を介して互いに通信するようになされている。また、通信システム100には、各ユーザに共通の公開パラメータPV (Public Values) が管理され

ている公開データベースPD (Public Database) が設けられている。

【0053】証明書発行者Q用端末装置20は、証明書発行者Q固有の秘密鍵 $s_Q$  (秘密情報) 及び公開鍵 $v_Q$  (公開情報) を生成する公開鍵生成部21と、秘密鍵 $s_Q$  及び公開パラメータPVを用いて平文mに対する署名 (匿名公開鍵証明書) を生成する署名生成部22とを備えている。

【0054】一方、ユーザ用端末装置30、40、50、・・・は、各々同様の構成としている。例えば、ユーザj用端末装置30は、ユーザj固有の秘密鍵 $s_j$  及び公開鍵 $v_j$  を生成する公開鍵生成部31と、平文mと上記署名の対応関係が正しいか否かを判別する判別部32と、新たな署名を生成する署名生成部33とを備えている。また、ユーザj用端末装置30は、新たな署名を確認する確認部35と、確認部35で確認された新たな署名を用いて平文を暗号化する暗号化部36と、確認部35で確認された新たな署名を用いて暗号文を復号する復号部34とを備えている。

【0055】以下、上述のような通信システム100の動作を上記図1及び図2を用いて説明する。尚、上記図2中の記号は、上記図5と同様の表記規則に従うものとする。

【0056】ステップS200：まず、通信システム100の共通のデータとして、大きな素数 $p$ 、 $Z_p^*$ の要素であり且つ位数 $p-1$ の $\alpha$ 、一方向性ハッシュ関数 $H_0: Z \rightarrow Z_p \setminus \{0\}$ を用いる。尚、 $p$ は、例えば、「 $p > 2^{512}$ 」とする。これらのパラメータ (公開パラメータPV (Public Values)) は、通信システム100に参加している全てのユーザがアクセスすることができ、且つ不当な改ざん等が起こらないように適切に管理されている公開データベースPD (Public Database) に登録されているものとする。そこで、証明書発行者 (authority) Q用端末装置20は、公開鍵生成部21により、秘密鍵 (復号鍵)  $s_Q$  ( $\in Z_{p-1}^*$ ) と、公開鍵 (暗号化鍵)  $v_Q$  ( $= \alpha s_Q \bmod p$ ) とを生成し、公開鍵 $v_Q$  を公開データベースPDに登録する。また、任意のユーザ用端末装置 (ここではユーザ (User) j用端末装置30とする) は、公開鍵生成部31により、秘密鍵 (復号鍵)  $s_j$  ( $\in Z_{p-1}^*$ ) と、公開鍵 (暗号化鍵)  $v_j$  ( $= \alpha s_j \bmod p$ ) とを生成し、公開鍵 $v_j$  を公開データベースPDに登録する。

【0057】ステップS201：匿名公開鍵証明書の生成

証明書発行者Q用端末装置20は、署名生成部22により、ユーザjの公開鍵 $v_j$  を、乱数 (random number)  $k$  を用いて変換した $r$ を求め、平文mに対する署名 (例えば、ElGamal暗号によるデジタル署名) を生成する。具体的には、署名生成部22は、乱数 (秘密の乱数)  $k$  ( $k \in Z_{p-1}^*$ ) を選択し、



$$r = v j^k \bmod p$$

$$s = (H_0(m) - s_0 \cdot r) \cdot k^{-1} \bmod (p-1)$$

なる計算を行う。この平文 $m$ に対するEIGamal暗号によるデジタル署名 $r, s$ が匿名公開鍵証明書である。また、平文 $m$ は、その匿名公開鍵証明書の種類を示すパラメータとして使用できる。尚、匿名公開鍵証明書の種類を示すパラメータとしては、平文 $m$ 或いは $H_0(m)$ の代わりに、予め決められた固定値を使用してもよい。

【0058】ステップS202：匿名公開鍵証明書の配送

次に、証明書発行者Q用端末装置20は、署名生成部22で生成したデジタル署名 $r, s$ と、その種類を示すパラメータ $m$ とを匿名公開鍵証明書 $(m, r, s)$ として、ユーザj用端末装置30に対して送信する。

【0059】ステップS203：これを受けたユーザj用端末装置30は、判別部32により、

$$s j' = s \cdot s j^{-1} \bmod (p-1)$$

を求め、

$$\alpha H_0(m) \equiv v q^r \cdot r s j' \pmod{p}$$

が成り立つことを確認する。

【0060】ステップS204：公開鍵暗号の利用

そして、ユーザj用端末装置30は、

$$\alpha H_0(m) \cdot v q^{-r} \equiv r s j' \pmod{p}$$

により、「 $r$ 」を底、「 $\alpha H_0(m) \cdot v q^{-r} \bmod p$ 」を公開鍵、「 $s j'$ 」を秘密鍵として、離散対数問題に基づく公開鍵暗号を利用する。

【0061】そこで、例えば、EIGamal暗号によるデジタル署名を利用する場合について説明する。

【0062】ステップS204(1)：デジタル署名の生成

ユーザj用端末装置30は、署名生成部33により、平文 $m'$ に対する署名を以下のようにして生成する。

①署名生成部33は、乱数 $k' (\in Z_{p-1}^*)$ を生成する。

②署名生成部33は、

$$r' = \alpha^{k'} \bmod p$$

を計算する。

③署名生成部33は、

$$s' = (H_0(m') - s j' \cdot r) \cdot (k')^{-1} \bmod (p-1)$$

を計算する。

④そして、ユーザj用端末装置30は、 $m'$ と、署名生成部33で得られた $r'$ 及び $s'$ を、証明書発行者Q用端末装置20からの匿名公開鍵証明書 $(m, r)$ と共に通信相手(ここではユーザi用端末装置40とする)に対して送信する。

【0063】ステップS204(2)：署名検証

これを受けたユーザi用端末装置40は、確認部45により、

$$r H_0(m') \equiv (\alpha H_0(m) \cdot v q^{-r}) r' \cdot (r') s' \pmod{p}$$

なる式が成立するかを確認する。そして、ユーザi用端末装置40は、この確認ができた場合に、 $m'$ に対する署名は証明書発行者Qによって選ばれたユーザによって生成された署名であることを認識する。

【0064】また、上述のステップS204：公開鍵暗号の利用としては、暗号化にも利用することができる。そこで、例えば、ユーザk用端末装置50において、EIGamal暗号による暗号化を行う場合について説明する。

【0065】暗号化：ユーザk用端末装置50は、暗号化部56により、平文 $m''$ を以下のようにして暗号化する。

①暗号化部56は、乱数 $k''$ を生成する。

②暗号化部56は、

$$C_1 = r k'' \bmod p$$

を計算する。

③暗号化部56は、

$$C_2 = m'' \cdot (\alpha H_0(m) \cdot v q^{-r} \bmod p) k'' \bmod p$$

を計算する。

④そして、ユーザk用端末装置50は、暗号化部56で得られた $C_1$ 及び $C_2$ を、ユーザj用端末装置30に対して送信する。

【0066】復号：これを受けたユーザj用端末装置30は、復号部34により、

$$m'' = C_2 / C_1 s j' \bmod p$$

なる計算を行って、平文 $m''$ を得る。

【0067】尚、上述のステップS204：公開鍵暗号の利用として、EIGamal暗号を用いたものを説明したが、これに限らず、離散対数問題に基づく公開鍵暗号等を用いたものにも利用することができる。

【0068】つぎに、第2の実施の形態について説明する。

【0069】この第2の実施の形態では、上述した第1の実施の形態における通信システム100に、EIGamal暗号のデジタル署名方式の変形版を適用する。このため、第1の実施の形態では、EIGamal暗号で $p-1$ を用いて法演算を行うのに対して、第2の実施の形態では、素数 $q$ ( $q$ は $p-1$ を割り切る)を用いて法演算を行うという点が異なる。

【0070】尚、この第2の実施の形態を実施する通信システム100の構成については、上述した第1の実施の形態と同様であるため、その詳細な説明は省略する。以下、第1の実施の形態と異なる点についてのみ、図3を用いて具体的に説明する。

【0071】ステップS300：先ず、通信システム100の共通のデータとして、大きな素数 $p, q$ ( $q$ は $p-1$ を割り切る)、 $Z_p^*$ の要素であり且つ位数 $q$ の $\alpha$ 、一方向性ハッシュ関数 $H_0: Z \rightarrow Z_q \setminus \{0\}$ 、 $H$

1:  $Z_q \times Z \rightarrow \{0, \dots, 2^t - 1\}$  を用いる。  
 尚、ここでは、例えば、「 $p > 2^{512}$ 」、「 $q > 2^{160}$ 」、「 $t > 72$ 」とする。これらのパラメータ（公開パラメータPV）は、通信システム100に参加している全てのユーザがアクセスすることができ、且つ不当な改ざん等が起こらないように適切に管理されている公開データベースPDに登録されているものとする。  
 そこで、証明書発行者Q用端末装置20は、公開鍵生成部21により、秘密鍵 $s_Q$  ( $\in Z_q \setminus \{0\}$ ) と、公開鍵 $v_Q$  ( $= \alpha^{s_Q} \bmod p$ ) とを生成し、公開鍵 $v_Q$  を公開データベースPDに登録する。また、任意のユーザ用端末装置（ここではユーザ（User）j用端末装置30とする）は、公開鍵生成部31により、秘密鍵 $s_j$  ( $\in Z_q \setminus \{0\}$ ) と、公開鍵 $v_j$  ( $= \alpha^{s_j} \bmod p$ ) とを生成し、公開鍵 $v_j$  を公開データベースPDに登録する。

【0072】ステップS301：匿名公開鍵証明書の生成

証明書発行者Q用端末装置20は、署名生成部22により、ユーザjの公開鍵 $v_j$  を、乱数（random number） $k$  を用いて変換した $r$  を求め、平文 $m$  に対する署名（例えば、ElGamal暗号によるデジタル署名）を生成する。具体的には、署名生成部22は、乱数（秘密の乱数） $k$  ( $k \in Z_q \setminus \{0\}$ ) を選択し、

$$r = v_j^k \bmod p$$

$$s = (H_0(m) - s_Q \cdot r) \cdot k^{-1} \bmod q$$

なる計算を行う。この平文 $m$  に対するElGamal暗号によるデジタル署名 $r, s$  が匿名公開鍵証明書である。また、平文 $m$  は、その匿名公開鍵証明書の種類を示すパラメータとして使用できる。尚、匿名公開鍵証明書の種類を示すパラメータとしては、平文 $m$  或いは $H_0(m)$  の代わりに、予め決められた固定値を使用してもよい。

【0073】ステップS302：匿名公開鍵証明書の配送

次に、証明書発行者Q用端末装置20は、署名生成部22で生成したデジタル署名 $r, s$  と、その種類を示すパラメータ $m$  とを匿名公開鍵証明書 $(m, r, s)$  として、ユーザj用端末装置30に対して送信する。

【0074】ステップS303：これを受けたユーザj用端末装置30は、判別部32により、

$$s_j' = s \cdot s_j^{-1} \bmod q$$

を求め、

$$\alpha^{H_0(m)} \equiv v_Q^r \cdot r \cdot s_j' \pmod{p}$$

が成り立つことを確認する。

【0075】ステップS304：公開鍵暗号の利用

そして、ユーザj用端末装置30は、

$$\alpha^{H_0(m)} \cdot v_Q^{-r} \equiv r s_j' \pmod{p}$$

により、「 $r$ 」を底、「 $\alpha^{H_0(m)} \cdot v_Q^{-r} \bmod p$ 」を公開鍵、「 $s_j'$ 」を秘密鍵として、離散対数問題に基づく公開鍵暗号を利用する。

【0076】そこで、例えば、Schonorr暗号によるデジタル署名を利用する場合について説明する。

【0077】ステップS304（1）：デジタル署名の生成

ユーザj用端末装置30は、署名生成部33により、平文 $m'$  に対する署名を以下のようにして生成する。

①署名生成部33は、乱数 $k'$  ( $\in Z_q \setminus \{0\}$ ) を生成する。

②署名生成部33は、

$$x = r^{k'} \bmod p$$

を計算する。

③署名生成部33は、

$$e = H_1(x, m')$$

を計算する。

④署名生成部33は、

$$y = k' - e \cdot s_j' \bmod q$$

を計算する。

⑤そして、ユーザj用端末装置30は、 $m'$  と、署名生成部33で得られた $e$  及び $y$  を、証明書発行者Q用端末装置20からの匿名公開鍵証明書 $(m, r)$  と共に通信相手（ここではユーザi用端末装置40とする）に対して送信する。

【0078】ステップS304（2）：署名検証  
 これを受けたユーザi用端末装置40は、確認部45により、

$$e = H_1(r^y \cdot (\alpha^{H_0(m')} \cdot v_Q^{-r})^e \bmod p, m')$$

なる式が成立するかを確認する。そして、ユーザi用端末装置40は、この確認ができた場合に、 $m'$  に対する署名は、証明書発行者Qによって選ばれたユーザによって生成された署名であることを認識する。

【0079】また、上述のステップS304：公開鍵暗号の利用としては、暗号化にも利用することができる。そこで、例えば、ユーザk用端末装置50において、ElGamal暗号による暗号化を行う場合について説明する。

【0080】暗号化：ユーザk用端末装置50は、暗号化部56により、平文 $m''$  を以下のようにして暗号化する。

①暗号化部56は、乱数 $k''$  を生成する。

②暗号化部56は、

$$C_1 = r^{k''} \bmod p$$

を計算する。

③暗号化部56は、

$$C_2 = m'' \cdot (\alpha^{H_0(m)} \cdot v_Q^{-r} \bmod p)^{k''} \bmod p$$

を計算する。

④そして、ユーザk用端末装置50は、暗号化部56で得られた $C_1$  及び $C_2$  を、ユーザj用端末装置30に対して送信する。

【0081】復号：これを受けたユーザj用端末装置30

0は、復号部34により、

$$m'' = C_2 / C_1 s_j' \bmod p$$

なる計算を行って、平文 $m''$ を得る。

【0082】尚、上述のステップS304：公開鍵暗号の利用として、Schnorr暗号やElGamal暗号を用いたものを説明したが、これに限らず、離散対数問題に基づく公開鍵暗号等を用いたものにも利用することができる。

【0083】つぎに、第3の実施の形態について説明する。

【0084】この第3の実施の形態では、上述した第1の実施の形態における通信システム100に、ElGamal暗号のデジタル署名方式の変形版を適用する。すなわち、第3の実施の形態では、第1の実施の形態と同様に、匿名公開鍵証明書において平文 $m$ （平文 $m$ を元に計算して得た $H_0(m)$ ）を用いる際に、 $H_0(m) = 0$ とする。

【0085】尚、この第3の実施の形態を実施する通信システム100の構成については、上述した第1の実施の形態と同様であるため、その詳細な説明は省略する。以下、第1の実施の形態と異なる点についてのみ、図4を用いて具体的に説明する。

【0086】ステップS400：まず、通信システム100の共通のデータとして、素数 $p$ 、 $Z_p^*$ の要素であり且つ位数 $p-1$ の $\alpha$ 、一方向性ハッシュ関数 $H_0 : Z \rightarrow Z_p \setminus \{0\}$ を用いる。尚、 $p$ は、例えば、「 $p > 2512$ 」とする。これらのパラメータ（公開パラメータ $PV$ ）は、通信システム100に参加している全てのユーザがアクセスすることができ、且つ不当な改ざん等が起こらないように適切に管理されている公開データベースPDに登録されているものとする。そこで、証明書発行者Q用端末装置20は、公開鍵生成部21により、秘密鍵 $s_Q (\in Z_{p-1}^*)$ と、公開鍵 $v_Q (= \alpha^{s_Q} \bmod p)$ とを生成し、公開鍵 $v_Q$ を公開データベースPDに登録する。また、任意のユーザ用端末装置（ここではユーザ（User）j用端末装置30とする）は、公開鍵生成部31により、秘密鍵 $s_j (\in Z_{p-1}^*)$ と、公開鍵 $v_j (= \alpha^{s_j} \bmod p)$ とを生成し、公開鍵 $v_j$ を公開データベースPDに登録する。

【0087】ステップS401：匿名公開鍵証明書の生成

証明書発行者Q用端末装置20は、署名生成部22により、ユーザjの公開鍵 $v_j$ を、乱数（random number） $k$ を用いて変換した $r$ を求め、ElGamal暗号のデジタル署名の変形版、例えば、平文 $m$ をハッシュ関数の入力とした結果が「0」となるElGamal暗号の署名を生成する。具体的には、署名生成部22は、乱数（秘密の乱数） $k (k \in Z_{p-1}^*)$ を選択し、

$$r = v_j^k \bmod p$$

$$s = s_Q \cdot r \cdot k^{-1} \bmod (p-1)$$

なる計算を行う。このデジタル署名 $r, s$ が匿名公開鍵証明書である。

【0088】ステップS402：匿名公開鍵証明書の配送次に、証明書発行者Q用端末装置20は、署名生成部22で生成したデジタル署名 $r, s$ を匿名公開鍵証明書 $(r, s)$ として、ユーザj用端末装置30に対して送信する。

【0089】ステップS403：これを受けたユーザj用端末装置30は、判別部32により、

$$s_j' = s \cdot s_j^{-1} \bmod (p-1)$$

を求め、

$$v_Q r \equiv r^{s_j'} \pmod{p}$$

が成り立つことを確認する。

【0090】ステップS404：公開鍵暗号の利用  
そして、ユーザj用端末装置30は、

$$v_Q r \equiv r^{s_j'} \pmod{p}$$

により、「 $r$ 」を底、「 $v_Q r \bmod p$ 」を公開鍵、

「 $s_j'$ 」を秘密鍵として、離散対数問題に基づく公開鍵暗号を利用する。

【0091】そこで、例えば、ElGamal暗号によるデジタル署名を利用する場合について説明する。

【0092】ステップS404（1）：デジタル署名の生成

ユーザj用端末装置30は、署名生成部33により、平文 $m'$ に対する署名を以下のようにして生成する。

①署名生成部33は、乱数 $k' (\in Z_{p-1}^*)$ を生成する。

②署名生成部33は、

$$r' = \alpha^{k'} \bmod p$$

を計算する。

③署名生成部33は、

$$s' = (H(m') - s_j' \cdot r) \cdot (k')^{-1} \bmod (p-1)$$

を計算する。

④そして、ユーザj用端末装置30は、 $m'$ と、署名生成部33で得られた $r'$ 及び $s'$ を、証明書発行者Q用端末装置20からの匿名公開鍵証明書 $(m, r)$ と共に通信相手（ここではユーザi用端末装置40とする）に対して送信する。

【0093】ステップS404（2）：署名検証  
これを受けたユーザi用端末装置40は、確認部45により、

$$r^{H_0(m')} \equiv (v_Q r')^{r'} \cdot (r')^{s'} \pmod{p}$$

なる式が成立するかを確認する。そして、ユーザi用端末装置40は、この確認ができた場合に、 $m'$ に対する署名は、証明書発行者Qによって選ばれたユーザによって生成された署名であることを認識する。

【0094】また、上述のステップS404：公開鍵暗号の利用としては、暗号化にも利用することができる。

そこで、例えば、ユーザk用端末装置50において、E

「Gamma」暗号による暗号化を行う場合について説明する。

【0095】暗号化：ユーザk用端末装置50は、暗号化部56により、平文 $m$ を以下のようにして暗号化する。

①暗号化部56は、乱数 $k$ を生成する。

②暗号化部56は、

$$C_1 = r k^r \bmod p$$

を計算する。

③暗号化部56は、

$$C_2 = m^r \cdot (v q^r \bmod p) k^r \bmod p$$

を計算する。

④そして、ユーザk用端末装置50は、暗号化部56で得られた $C_1$ 及び $C_2$ を、ユーザj用端末装置30に対して送信する。

【0096】復号：これを受けたユーザj用端末装置30は、復号部34により、

$$m^r = C_2 / C_1^{s_j} \bmod p$$

なる計算を行って、平文 $m$ を得る。

【0097】尚、上述のステップS404：公開鍵暗号の利用として、E「Gamma」暗号を用いたものを説明したが、これに限らず、離散対数問題に基づく公開鍵暗号等を用いたものにも利用することができる。

【0098】上述のように、本発明においては、 $p$ は素数、 $\alpha$ の位数は $p-1$ 、 $r \equiv v_j k \equiv \alpha^{s_j k} \pmod{p}$ であり、 $s_j \in \mathbb{Z}_{p-1}^*$ 、 $k \in \mathbb{Z}_{p-1}^*$ である。或いは、 $p$ と $q$ が素数で、 $q$ は $p-1$ を割り切り、 $\alpha$ の位数が $q$ 、 $r \equiv v_j k \equiv \alpha^{s_j k} \pmod{p}$ であり、 $s_j \in \mathbb{Z}_q \setminus \{0\}$ 、 $k \in \mathbb{Z}_q \setminus \{0\}$ である。したがって、任意の $r$ が与えられたとき、その $r$ は、どのユーザの公開鍵からも計算して得ることができる値であり、実際に使用された $k$ の値が分からない限りは、どのユーザの公開鍵から計算して得られたのかは全く特定することができない。換言すれば、匿名公開鍵証明書である署名 $r$ には、どのユーザの匿名公開鍵証明書であるかを特定するための情報が一切含まれない。これにより、計算量的な上述した仮定2によってではなく、情報量的に匿名性が実現されており、仮定2が成り立たなくなる事態が起きたとしても、匿名性を確実に保つことができる。このため、プライバシー保護に関する安全性を向上させることができる。

【0099】また、上述した何れの実施の形態においても、以下のように運用することで、プライバシー保護に関する安全性をさらに向上させることができる。

①証明書発行者Q用端末装置20は、任意のユーザ用端末装置（例えば、ユーザj用端末装置30）に対して毎回異なる乱数 $k$ を用いた匿名公開鍵証明書を生成してユーザj用端末装置30に対して送信する。

②これを受けたユーザj用端末装置30は、デジタル署名を生成せずに、1つの匿名公開証明書を異なる平文に対して使用する。このような、匿名公開鍵証明書を使用する方式（One-time Certificates、使い捨て証明書方式）により、任意のデジタル署名を生成したユーザと、それとは別のデジタル署名を生成したユーザとが、同一のユーザであるか否かを判別することは、証明書発行者Qと、上記任意のデジタル署名を生成したユーザ以外のユーザとにとって、情報量的に非常に困難、すなわち不可能である。したがって、ユーザの匿名性は情報量的に保たれるため、プライバシー保護に関する安全性をさらに向上させることができる。

【0100】

【発明の効果】以上説明したように本発明によれば、匿名公開鍵証明書である署名には、どのユーザの匿名公開鍵証明書であるかを特定するための情報が一切含まれない。これにより、計算量的な上述した仮定2によってではなく、情報量的に匿名性が実現されており、仮定2が成り立たなくなる事態が起きたとしても、匿名性を確実に保つことができる。したがって、プライバシー保護に関する安全性を向上させることができる。

【図面の簡単な説明】

【図1】第1の実施の形態において、本発明に係る情報通信システムを適用した通信システムの構成を示すブロック図である。

【図2】上記通信システムにおけるデジタル署名方式を説明するための図である。

【図3】第2の実施の形態において、上記通信システムにおけるデジタル署名方式を説明するための図である。

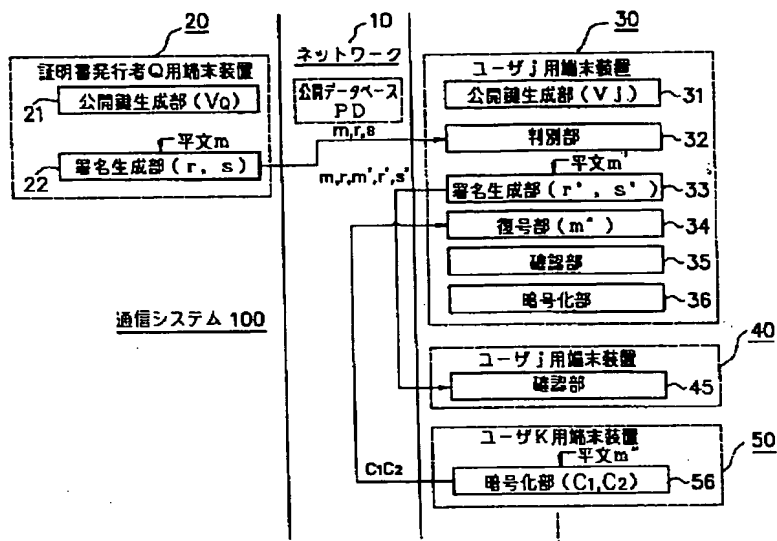
【図4】第3の実施の形態において、上記通信システムにおけるデジタル署名方式を説明するための図である。

【図5】従来のデジタル署名方式を説明するための図である。

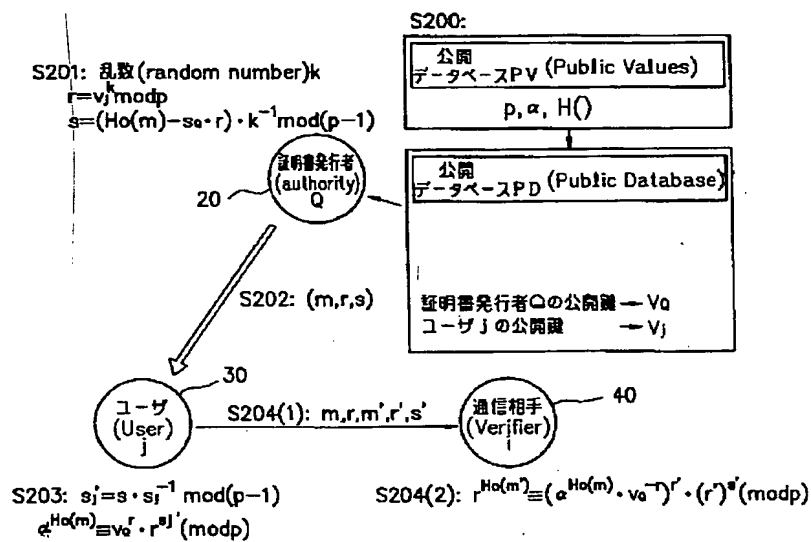
【符号の説明】

- 10 ネットワーク
- 20 証明書発行者用端末装置
- 21 公開鍵生成部
- 22 署名生成部
- 30～50 ユーザ用端末装置
- 31 公開鍵生成部
- 32 判別部
- 33 署名生成部
- 34 復号部
- 35、45 確認部
- 36、56 暗号化部

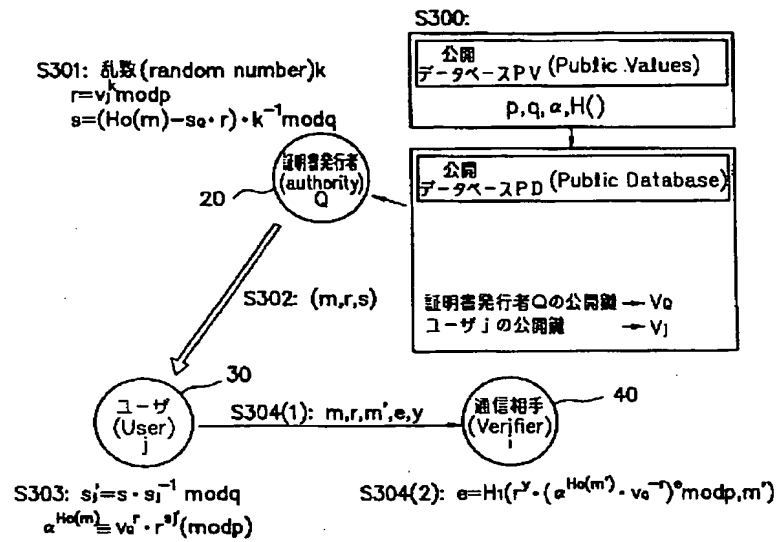
【図 1】



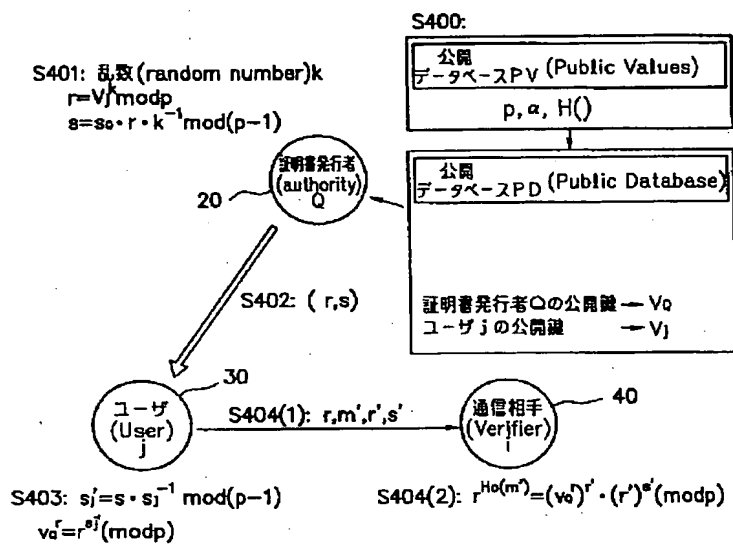
【図 2】



【図 3】



【図 4】



【図 5】

